ABSTRACT OF THE DISCLOSURE

The present invention provides an apparatus and method for performing cryptographic operations on a plurality of input data blocks within a processor, where the size of the input data blocks is programmable. In one embodiment, an apparatus for performing cryptographic operations is provided. The apparatus includes a cryptographic instruction and execution logic. The cryptographic instruction is received by a computing device as part of an instruction flow executing on the computing device. The cryptographic instruction prescribes one of the cryptographic operations, and also one of a plurality of data block sizes. The execution logic is operatively coupled to the cryptographic instruction. The execution logic executes the one of the cryptographic operations. The execution logic has a block size controller that employs the one of a plurality of data block sizes during execution of the one of the cryptographic operations.